kaspersky AKTYWUJ PRZYSZŁOŚĆ

Kaspersky Endpoint Detection and Response Optimum

Podnieś ochronę punktów końcowych na wyższy poziom i z łatwością pokonuj zagrożenia unikające wykrycia.

Nadszedł czas, aby wspiąć się na wyższy poziom. Teraz możesz nie tylko chronić swoją organizację przed szkodliwym oprogramowaniem za pomocą popularnych technologii. Masz także możliwość identyfikowania, analizowania i skutecznego neutralizowania zagrożeń, których celem jest unikanie tradycyjnych rozwiązań bezpieczeństwa i zagnieżdżanie się głęboko w systemach. Zagrożeń, które są gotowe zrobić to, co najgorsze.

W około **30% udanych ataków** cyberprzestępcy używają legalnych narzędzi systemowych do uruchamiania niebezpiecznych skryptów i programów, pobierania szkodliwych funkcji, skanowania sieci i uzyskiwania zdalnego dostępu do zainfekowanego urządzenia.
Raport z analizy reagowania na incydenty, Kaspersky, 2020 r.

Wyzwania

Większe zakłócenia

Szkodliwe programy, ransomware, narzędzia szpiegujące i inne zagrożenia coraz lepiej unikają wykrycia, a przeprowadzanie ataków jest coraz tańsze. W efekcie ryzyko doświadczenia poważnego ataku jest większe niż kiedykolwiek wcześniej, podobnie jak rozmiar szkód i zakłóceń w funkcjonowaniu biznesu.

Skomplikowana infrastruktura

Obecnie zdecydowana większość menedżerów IT i specjalistów ds. bezpieczeństwa musi chronić całą gamę różnych punktów końcowych – laptopów, serwerów, środowisk wirtualnych i chmurowych oraz zdalnych, a także stacji roboczych – a jednocześnie radzić sobie z trudnym w kontrolowaniu złożonym środowiskiem IT.

Utrzymanie równowagi

Cyberbezpieczeństwo polega w dużej mierze na znalezieniu optymalnej równowagi między dostępnymi zasobami, a najwyższym osiągalnym poziomem ochrony. Tymczasem czas specjalistów IT jest jednym z najrzadszych zasobów.

Rozwiązanie

Kaspersky Endpoint Detection and Response (EDR) Optimum pomaga identyfikować, analizować i neutralizować zagrożenia unikające wykrycia, zapewniając łatwe w zastosowaniu zaawansowane wykrywanie, uproszczoną analizę i zautomatyzowane reagowanie na cyberincydenty.

Nawet w przypadku udanych ataków straty finansowe były o **32% niższe**, jeśli na naruszenie zareagowano szybko.
Raport z analizy reagowania na incydenty, Kaspersky, 2020

Kompletne wyposażenie i gotowość do działania

W oparciu o zaawansowane mechanizmy wykrywania, w tym uczenie maszynowe i ulepszoną analizę podejrzanych działań, Kaspersky EDR Optimum zapewnia szczegółowy wgląd w zagrożenia, proste narzędzia analityczne i dochodzeniowe oraz automatyczne reagowanie. Będziesz w stanie zobaczyć zagrożenie, zrozumieć je, ujawnić jego pełny zakres i podjąć natychmiastową reakcję, zapobiegając przerwom w funkcjonowaniu Twojej firmy.

Jedno rozwiązanie

Kaspersky EDR Optimum wprowadza zaawansowane funkcje wykrywania, analizy i reagowania do ekosystemu bezpieczeństwa firmy Kaspersky, wzmacniając ochronę na wszystkich punktach końcowych: laptopach, serwerach, zasobach chmurowych i środowiskach wirtualnych. Scentralizowane wdrażanie i ujednolicone zarządzanie rozwiązaniem Kaspersky EDR Optimum może się odbywać w dwóch modelach: w chmurze lub lokalnie.

Łatwość użytkowania i wydajność

Kaspersky EDR Optimum jest przeznaczony dla mniejszych zespołów ds. cyberbezpieczeństwa o ograniczonych zasobach, które chcą poszerzyć swoje możliwości reagowania na incydenty. Wydajność jest zoptymalizowana pod kątem maksymalnej skuteczności i minimalnego angażowania ludzi, a czas specjalistów ds. bezpieczeństwa jest efektywnie wykorzystany dzięki automatyzacji i centralizacji wszystkich operacji administracyjnych oraz usprawnieniu przepływu pracy.

Kluczowe korzyści

- Ochrona przed coraz bardziej destrukcyjnymi zagrożeniami, które unikają wykrycia
- Ochrona wszystkich punktów końcowych: laptopów, serwerów czy zasobów chmurowych
- Pełna widoczność każdego zagrożenia w całej sieci
- Możliwość poznania podstawowej przyczyny i sposobu pojawienia się zagrożenia
- Ograniczenie dalszych szkód dzięki szybkiej reakcji podejmowanej automatycznie
- Oszczędność czasu i zasobów dzięki łatwości użytkowania i automatyzacji

Najważniejsze przypadki użycia EDR

Zaawansowane wykrywanie

Identyfikowanie zagrożeń unikających wykrycia wymaga wielu mechanizmów:

- Wykrywanie zagrożeń na podstawie ich zachowania oraz zapobieganie exploitom oparte na uczeniu maszynowym
- Heurystyka, inteligentne wpisy w bazie danych i inne technologie oparte na sztucznej inteligencji
- Wbudowany emulator do wykrywania szkodliwego zachowania, zanim zostanie ono uruchomione
- Piaskownica pozwalająca na precyzyjną analizę zachowania (dostępna w postaci Kaspersky Sandbox)
- Dane dotyczące globalnych zagrożeń gromadzone i analizowane w laboratorium przez systemy oparte na sztucznej inteligencji, przy wsparciu wiedzy ekspertów

Odpowiedzi na kluczowe pytania

Zagrożenia unikające wykrycia powinny zostać dogłębnie zbadane, a następnie w pełni wyeliminowane. Rozwiązanie EDR pomaga znaleźć odpowiedzi na następujące pytania:

- Czy firma jest teraz atakowana?
- Czy dany branżowy atak dotarł do infrastruktury firmy?
- Skąd wzięło się dane zagrożenie?
- Co udało mu się zrobić na firmowych komputerach?
- Czy są jakieś ukryte warstwy tego zagrożenia?
- Czy inne punkty końcowe też zostały dotknięte?

Szybkie reagowanie

Reagowanie na zagrożenia tuż po ich wykryciu – za pomocą jednego kliknięcia lub przy użyciu automatycznych działań:

- Blokada możliwości uruchamiania i rozprzestrzeniania się szkodliwego pliku w sieci podczas analizy lub po jej zakończeniu
- Automatyczna kwarantanna plików związanych z zagrożeniami, które unikają wykrycia, na wszystkich punktach końcowych
- Automatyczne izolowanie zainfekowanych urządzeń po wykryciu wskaźnika naruszenia (IoC) powiązanego z szybko rozprzestrzeniającym się zagrożeniem

Teraz możesz zrobić o wiele więcej

Dzięki zaawansowanym mechanizmom wykrywania opartym na uczeniu maszynowym masz wgląd we wszystkie szczegóły dotyczące każdego zagrożenia oraz sposób jego ewolucji na punktach końcowych. Ponadto masz pewność, że wszystkie zagrożenia zostały w pełni zneutralizowane i nie ukrywają się w systemie, szukając sposobności na wyrządzenie szkód.

Zabezpiecz infrastruktury hybrydowe

Infrastruktury hybrydowe dają wiele korzyści, jednak jednocześnie niosą ze sobą unikatowe wyzwania związane z bezpieczeństwem. Teraz, dzięki podstawowym funkcjom EDR, możesz usprawnić ochronę danych dla wirtualnych i fizycznych serwerów, zwirtualizowanych stacji roboczych oraz zasobów w chmurach publicznych.

Uwolnij się od natłoku alertów i w pełni wykorzystaj swoje zasoby dzięki scentralizowanemu zarządzaniu wszystkimi hybrydowymi punktami końcowymi oraz usprawnionemu przepływowi pracy EDR. Do zarządzania możesz wykorzystać platformę działającą w chmurze lub lokalnie w Twojej sieci.

Analizuj zagrożenia

Każdy alert zawiera informacje o wykrytym zagrożeniu i szczegóły dotyczące ścieżki rozprzestrzeniania się ataku. Dzięki temu możesz szybko przeprowadzić analizę i podjąć świadomą decyzję – czy zareagować za pomocą „pojedynczego kliknięcia", czy wybrać zautomatyzowane obsłużenie incydentu.

W celu identyfikowania w całej infrastrukturze konkretnych zagrożeń unikających wykrycia możesz importować wskaźniki IoC z zaufanych źródeł lub generować je w procesie śledztwa cyfrowego.

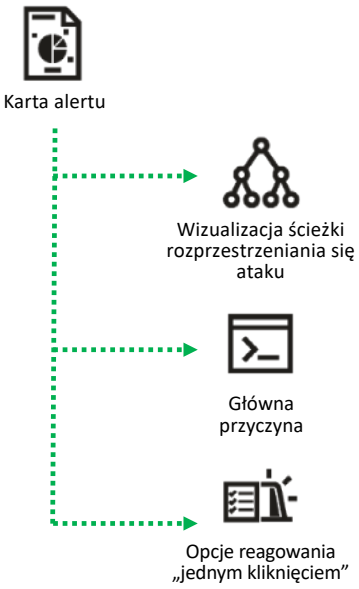
Zautomatyzuj reagowanie

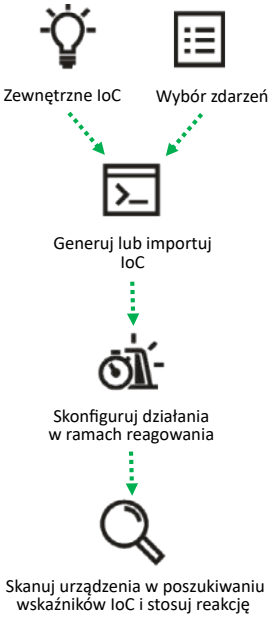
Reaguj błyskawicznie na zagrożenia podczas prowadzonego śledztwa cyfrowego. Możesz wybrać opcję „pojedynczego kliknięcia" dostępną w alercie dotyczącym incydentu lub skonfigurować automatyczne reagowanie w oparciu o wskaźniki IoC. Do działań podejmowanych w ramach reagowania należą:

- Izolowanie hosta
- Umieszczanie pliku w kwarantannie
- Blokowanie uruchamiania
- Uruchamianie skanowania obszarów krytycznych

Wielopoziomowa ochrona punktów końcowych

Technologie EDR mogą skutecznie funkcjonować tylko w połączeniu z silną, wielopoziomową ochroną na punktach końcowych. Dzięki takiemu podejściu nie tracisz czasu na powszechne zagrożenia i incydenty, które są automatycznie usuwane przez oprogramowanie zabezpieczające. W tym celu Kaspersky EDR Optimum współpracuje z jedną z naszych najczęściej testowanych i nagradzanych1 platform ochrony punktów końcowych: Kaspersky Endpoint Security for Business lub Kaspersky Hybrid Cloud Security.

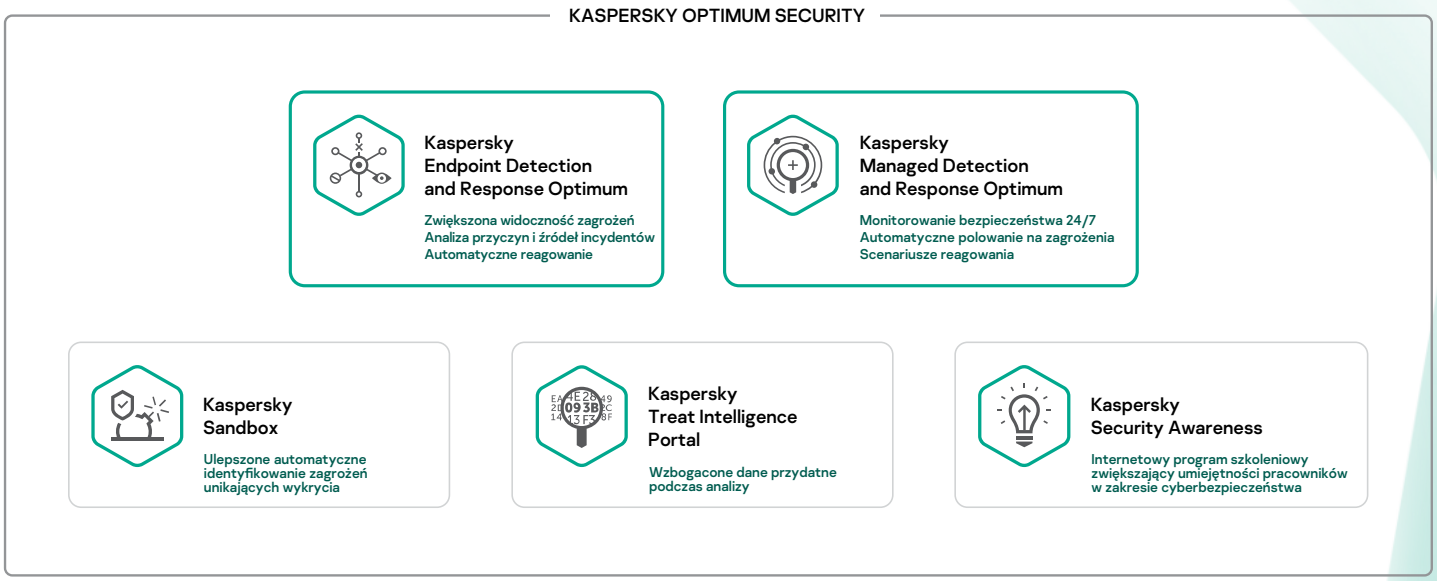




[1] https://www.kaspersky.pl/top3

Twoja platforma Kaspersky Optimum Security

EDR jest częścią ekosystemu obejmującego wiele technologii, narzędzi i usług. Kaspersky EDR Optimum jest kluczowym komponentem Kaspersky Optimum Security — szerszego rozwiązania wzmacniającego wiele aspektów ochrony przed zagrożeniami unikającymi wykrycia, przy jednoczesnej dbałości o oszczędne wykorzystanie zasobów:



Podejście krok po kroku

Kaspersky Optimum Security bazuje na platformie Kaspersky Security Foundations. Z kolei dzięki usługom Kaspersky Expert Security możesz w dowolnym momencie zacząć płynne wdrażanie potężnych narzędzi, które chronią przed najbardziej zaawansowanymi zagrożeniami.

Kaspersky Security Foundations

Automatycznie blokuj większość zagrożeń.

- Wielowektorowe zautomatyzowane zapobieganie typowym incydentom, stanowiącym zdecydowaną większość wszystkich cyberataków
- Podstawowy etap budowania zintegrowanej strategii ochronnej dla organizacji o dowolnej wielkości i złożoności
- Niezawodna ochrona punktów końcowych dla firm z małymi zespołami IT, które dopiero nabywają wiedzę specjalistyczną w zakresie bezpieczeństwa

Kaspersky Optimum Security

Zbuduj swoją ochronę przed zagrożeniami unikającymi wykrycia. Rozwiązanie idealne dla firm z:

- Niewielkim zespołem ds. bezpieczeństwa IT i z podstawową wiedzą z zakresu cyberbezpieczeństwa
- Środowiskiem IT, które się rozrasta i jest coraz bardziej złożone, co zwiększa powierzchnię ataku
- Brakiem zasobów cyberbezpieczeństwa i potrzebą zwiększonej ochrony
- Coraz większą potrzebą rozwijania zdolności reagowania na incydenty Kaspersky Expert Security

Kaspersky Expert Security

Przygotuj się na złożone ataki typu APT. Dla firm, które:

- Mają rozbudowane i rozproszone środowiska IT
- Dysponują dojrzałym zespołem ds. bezpieczeństwa IT lub ustabilizowanym Centrum Operacji Bezpieczeństwa (SOC)
- Nie chcą ryzykować ze względu na wyższe koszty incydentów bezpieczeństwa i naruszeń danych
- Mają problem z zapewnieniem zgodności z regulacjami

Aby dowiedzieć się więcej o tym, jak Kaspersky Endpoint Detection and Response Optimum radzi sobie z cyberzagrożeniami, jednocześnie dbając o Twój zespół ds. bezpieczeństwa i zasoby, odwiedź stronę https://vs.kaspersky.pl/download/dokumenty/kesb/Endpoint-Detection-and-Response-Optimum-Broszura.pdf.

Najnowsze informacje: www.kaspersky.pl/nowosci
Oficjalny blog: www.kaspersky.pl/blog

www.kaspersky.pl